

REMARKS

This Application has been carefully reviewed in light of the Final Office Action mailed July 15, 2005 (the "Office Action"). Claims 1-19 are pending in the application. The Examiner rejects Claims 1-19. To advance prosecution of this case, Applicants amend Claims 1-5, 7-16, and 18-19. In addition, Applicants cancel Claims 6 and 17 and add new Claims 20-33. Applicants do not admit that any amendments are necessary due to any prior art. Applicants respectfully request reconsideration and allowance of all pending claims.

Section 102 Rejections

The Examiner rejects Claims 1-9 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,826,013 issued to Nachenberg, et al. ("*Nachenberg*"). Applicants respectfully request reconsideration and allowance of Claims 1-5, 7-16 and 18-19.

Claim 1

Nachenberg fails to teach, suggest, or disclose several aspects of amended Claim 1. First, this reference fails to teach, suggest, or disclose "detecting at least one unused or misused operand or operator of the first predetermined number of instructions" as recited, in part, in amended Claim 1. Second, there is nothing in *Nachenberg* that teaches, suggests, or discloses "determining a probability" as recited, in part, in amended Claim 1. Third, the cited reference fails to teach, suggest, or disclose "an heuristic analysis of the collected information" as recited, in part, in amended Claim 1.

First, *Nachenberg* fails to teach, suggest, or disclose "detecting at least one unused or misused operand or operator of the first predetermined number of instructions" as recited, in part, in amended Claim 1. *Nachenberg* discloses a module for detecting polymorphic viruses by emulating instructions of a computer program. (*Nachenberg*; col. 3, ll. 6-7). In particular, the module in *Nachenberg* stores profiles of known polymorphic viruses. (*Nachenberg*, col. 8, ll. 24-27). As each instruction is emulated, the module compares the emulated instruction with the profiles of known polymorphic viruses. (*Nachenberg*, col. 8, ll. 24-27). Each profile that does not implement the emulated instruction is eliminated from further consideration. (*Nachenberg*, col. 8, ll. 27-31). When all profiles are eliminated from consideration, the module in *Nachenberg* compares virtual memory pages that were modified during emulation of the instructions with signatures of known polymorphic viruses. (*Nachenberg*; col. 10, ll. 13-18). Thus, the method in *Nachenberg* uses profiles of known

polymorphic viruses “rather than heuristic stopper and booster code sequences.” (*Nachenberg*; col. 3, ll. 5-6). Unlike the method of eliminating profiles disclosed in *Nachenberg*, the method of amended Claim 1 comprises “detecting at least one unused or misused operand or operator of the first predetermined number of instructions” as recited, in part, in amended Claim 1. There is nothing in *Nachenberg* that teaches, suggests, or discloses “detecting at least one unused or misused operand or operator” as recited, in part, in amended Claim 1. Because *Nachenberg* fails to teach, suggest, or disclose this aspect of amended Claim 1, *Nachenberg* does not support the rejection.

Second, the cited reference fails to teach, suggest, or disclose “determining a probability” as recited, in part, in amended Claim 1. As described above, the module in *Nachenberg* compares each emulated instruction with stored profiles of known polymorphic viruses. (*Nachenberg*, col. 8, ll. 24-27). Each profile that does not implement the emulated instruction is eliminated from further consideration. (*Nachenberg*, col. 8, ll. 27-31). When all profiles are eliminated, the module compares virtual memory pages that were modified during emulation with signatures of known polymorphic viruses. (*Nachenberg*; col. 10, ll. 13-18). Thus, the method in *Nachenberg* detects polymorphic viruses by comparing and eliminating profiles. *Nachenberg*, however, makes no reference to “determining a probability” as recited, in part, in amended Claim 1. Because the cited reference fails to teach, suggest, or disclose this aspect of amended Claim 1, the reference does not support the rejection.

Third, *Nachenberg* fails to teach, suggest, or disclose “an heuristic analysis of the collected information” as recited, in part, in amended Claim 1. As explained above, the module in *Nachenberg* compares each emulated instruction with the stored profiles of known polymorphic viruses. (*Nachenberg*, col. 8, ll. 24-27). When all profiles are eliminated from consideration, the module in *Nachenberg* compares modified virtual memory pages with signatures of known polymorphic viruses. (*Nachenberg*; col. 10, ll. 13-18). Thus, *Nachenberg* uses “mutation-engine specific information for each known polymorphic virus *rather than heuristic stopper and booster code sequences.*” (*Nachenberg*; col. 3, ll. 4-6) (emphasis added). According to *Nachenberg*, the disclosed technique “reduces the number of instructions emulated prior to scanning the remaining target files *without resort to booster or stopper heuristics.*” (*Nachenberg*; col. 3, ll. 51-53) (emphasis added). Thus, *Nachenberg* discloses a method that specifically omits any heuristic analysis. There is nothing in

Nachenberg that teaches, suggests, or discloses “an heuristic analysis of the collected information” as recited, in part, in amended Claim 1. Because the cited reference fails to teach, suggest, or disclose this aspect of amended Claim 1, the cited reference does not support the rejection. For at least these reasons, Applicants respectfully request reconsideration and allowance of amended Claim 1.

Claims 2-5, 7-8

Amended Claims 2-5 and 7-8 depend from amended Claim 1, shown above to be allowable. In addition, amended Claims 2-5 and 7-8 recite further elements not taught, suggested, or disclosed by *Nachenberg*. First, the cited reference fails to teach, suggest, or disclose “emulating additional instructions if the determined probability is above a predetermined threshold” as recited, in part, in amended Claim 2. Second, there is nothing in *Nachenberg* that teaches, suggests, or discloses “determining, for each of the plurality of registers and/or flags, a number of times that the register and/or flag was improperly used” as recited, in part, in amended Claim 5.

First, *Nachenberg* fails to teach, suggest, or disclose “emulating additional instructions if the determined probability is above a predetermined threshold” as recited, in amended Claim 2. As explained above, there is nothing in *Nachenberg* that teaches, suggests, or discloses a “determined probability” as recited, in part, in amended Claim 2. Furthermore, *Nachenberg* makes no mention of a probability being above “a predetermined threshold” as recited, in part, in amended Claim 2. Because the cited reference fails to teach, suggest, or disclose these aspects of amended Claim 2, the cited reference does not support the rejection.

Second, *Nachenberg* fails to teach, suggest, or disclose “determining, for each of the plurality of registers and/or flags, a number of times that the register and/or flag was improperly used” as recited, in part, in amended Claim 5. The module in *Nachenberg* flags profiles of known viruses that do not use the emulated instructions. (*Nachenberg*; col. 3, ll. 37-53). There is nothing, however, in *Nachenberg* that teaches, suggests, or discloses “determining, for each of the plurality of registers and/or flags, *a number of times* that the register and/or flag was improperly used” as recited, in part, in amended Claim 5. (Emphasis added). Because *Nachenberg* fails to teach, suggest, or disclose this aspect of amended Claim 5, the rejection is improper.

For at least these reasons, Applicants respectfully request reconsideration and allowance of amended Claims 2-5 and 7-8.

Claims 9-12

In rejecting Claims 9-12, the Examiner employs the same rationale used to reject Claim 1. Accordingly, for at least the reasons stated with respect to amended Claim 1, Applicants respectfully request reconsideration and allowance of amended Claims 9-12.

Claims 13-16, 18-19

Amended Claims 13-16 and 18-19 depend from amended Claim 12, shown above to be allowable. In addition, amended Claims 13-16 and 18-19 recite further elements not taught, suggested, or disclosed by *Nachenberg*. For at least these reasons, Applicants respectfully request reconsideration and allowance of amended Claims 13-16 and 18-19.

CONCLUSION

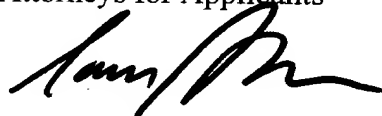
Applicants have made an earnest attempt to place this case in condition for allowance. For the foregoing reasons and for other reasons clearly apparent, Applicants respectfully request reconsideration and full allowance of all pending claims.

If there are matters that can be discussed by telephone to further the prosecution of this Application, Applicants invite the Examiner to call the undersigned attorney at (214) 953-6581 at the Examiner's convenience.

Because Applicants add new Claims 20-33, enclosed is check no. 125458 in the amount of \$600.00. The Commissioner is hereby authorized to charge any fees or credit any overpayment to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicants



Samir A. Bhavsar
Reg. No. 41,617

Date: September 15, 2005

Correspondence Address:

at Customer No. **05073**